AMENDMENTS TO THE SPECIFICATION

Please amend the Specification pursuant to 37 C.F.R. § 1.121 as follows:

I. Please insert the following paragraph before the first line of the Specification:

Cross-Reference to Related Applications

This application is a U.S. National Stage Application under 35 U.S.C. §371 of PCT International Application No. PCT/EP00/06510, filed July 10, 2000, which claims priority to German Patent Application No. DE 199 38 198.4, filed August 12, 1999. Each of these applications is incorporated herein by reference as if set forth in its entirety.

II. Please amend paragraph 0002 on page 1 of the Specification as follows:

Encryption methods of varied types belong to state of the art and increasingly have commercial importance. They are used for sending messages over commonly accessible transmission media, but only the owners of a cryptokey ~~being~~ are able to read these messages in plain text.

III. Please amend paragraph 0016 on page 4 of the Specification as follows:

In the following, the operating principle of the method will be explained in greater detail. The defined subscribers of the method are denoted by T1-Tn and each individual, that is not specifically named a subscriber is denoted by Ti. All other subscribers involved in the method are denoted by Tj except for the respective subscriber Ti. The publicly known components of the method are a publicly known mathematical group G, preferably the multiplicative group of all integral numbers modulo a large prime number p, and an element g of group G, preferably a number $0 < g < p$ having large multiplicative order. However, it is also possible to use other suitable mathematical structures for group G, for example, the multiplicative group of a finite body or the

group of the points of an elliptical curve. In the following, the method will be described on the basis of the group of numbers modulo a prime number p.

IV. Please amend paragraph 0018 on page 5 of the Specification as follows:

In the second method step, each subscriber Ti computes a common transmission key $k^{ij} := (g^{zi})^{zi}$ from received message g^{zj} for each further subscriber Tj, where $i \neq j$. Since $k^{ij} = [[k^{ij}]]$ k^{ji} applies, subscribers Ti and Tj now know a common transmission key k^{ij} and can therefore communicate confidentially.

V. Please amend paragraph 0021.2 on page 5 of the Specification as follows:

Referring to Fig. 1, in a method according to the present invention for establishing a common key within a group of subscribers, by each subscriber Ti of the at least three subscribers a respective message $Ni = (g^{zi} \bmod p)$ is generated from a publicly known element g of large order of a publicly known mathematical group G and a respective random number zi and the respective message is sent from the respective subscriber to all other subscribers Tj of the at least three subscribers (see block 102). Each respective random number zi is selected or generated by the respective subscriber Ti. Then, by each subscriber Ti, a transmission key k^{ij} is generated from the messages Nj received from the other subscribers Tj, $j \neq i$, and the respective random number zi according to $k^{ij} := Nj^{zi} = (g^{zj})^{zi}$ (see block 104). By each subscriber Ti, the respective random number zi is sent in encrypted form to all other subscribers Tj by generating the message Mij according to Mij := $E(k^{ij}, zi)$, where $E(k^{ij}, zi)$ ~~being is~~ a symmetrical encryption algorithm in which the data record zi is encrypted with the transmission key k^{ij} (see block 106). Finally, a common key k is determined by each subscriber Ti using the respective random number zi and the random

numbers zj, j ≠ i, received from the other subscribers according to k: = f(z1, ..., zn), where f ~~being~~ is a symmetrical function which is invariant under a permutation of its arguments (see block 108).

VI. Please amend paragraph 0024 on page 6 of the Specification as follows:

The method according to the present invention is executed according to the following method steps:

1. Subscriber A sends Na = g^{za} mod p to subscribers B and C, subscriber B sends Nb = g^{zb} mod p to subscribers A and C, and subscriber C sends Nc = g^{zc} mod p to subscribers A and B.

2. Subscriber A computes kab = Nb^{za} mod p and kac = Nc^{za} mod p. Subscribes B and C proceed analogously.

3. Subscriber A sends message Mab = E(kab, za) to subscriber B and message Mac = E(kac, za) to subscriber C. Here, E(k, m) denotes the symmetrical encryption of the data record with algorithm E under transmission key k^{ij}. ~~Subscribes~~ Subscribers B and C proceed analogously.

VII. Please amend paragraph 0026 on page 6 of the Specification as follows:

A variant of the method is to assign a special role to one of subscribers T1-Tn for the execution of the second method step. If this role is assigned, for example, to subscriber T1, then method steps 2 and 3 ~~or b and c~~ are executed only by subscriber T1. In fourth method step ~~d~~, all subscribers T1-Tn involved in the method compute common key k according to the assignment k: = h(z1, g^{z2}, ..., g^{zn}), it being required for h(x1, x2, ..., xn) to be a function which is symmetrical in arguments x2, ... xn. This variant drastically reduces the number of messages to be sent. An example of such a function g is, for instance,

$$k: = h(z1, g^{z2}, ..., g^{zn}) = g^{z1 \cdot z1} \cdot g^{z2 \cdot z1} \cdots g^{zn \cdot z1}.$$